arXiv:quant-ph/0504033v3 29 Jul 2005

# Higher order perturbation theory for decoherence in Grover's algorithm

Hiroo Azuma*

Research Center for Quantum Information Science,

Tamagawa University Research Institute,

6-1-1 Tamagawa-Gakuen, Machida-shi, Tokyo 194-8610, Japan

E-mail: h-azuma@lab.tamagawa.ac.jp

July 29, 2005

**Abstract**

In this paper, we study decoherence in Grover's quantum search algorithm using a perturbative method. We assume that each two-state system (qubit) that belongs to a register suffers a phase flip error ($\sigma_z$ error) with probability $p$ independently at every step in the algorithm, where $0 \leq p \leq 1$. Considering an $n$-qubit density operator to which Grover's iterative operation is applied $M$ times, we expand it in powers of $2Mnp$ and derive its matrix element order by order under the large-$n$ limit. [In this large-$n$ limit, we assume $p$ is small enough, so that $2Mnp$ can take any real positive value or zero. We regard $x \equiv 2Mnp(\geq 0)$ as a perturbative parameter.] We obtain recurrence relations between terms in the perturbative expansion. By these relations, we compute higher orders of the perturbation efficiently, so that we extend the range of the perturbative parameter that provides a reliable analysis. Calculating the matrix element numerically by this method, we derive the maximum value of the perturbative parameter $x$ at which the algorithm finds a correct item with a given threshold of probability $P_{\rm th}$ or more. (We refer to this maximum value of $x$ as $x_{\rm c}$, a critical point of $x$.) We obtain a curve of $x_{\rm c}$ as a function of $P_{\rm th}$ by repeating this numerical calculation for many points of $P_{\rm th}$ and find the following facts: a tangent of the obtained curve at $P_{\rm th} = 1$ is given by $x = (8/5)(1 - P_{\rm th})$, and we have $x_{\rm c} > -(8/5)\log_e P_{\rm th}$ near $P_{\rm th} = 0$.

## 1 Introduction

Many researchers think that decoherence is one of the most serious difficulties in realizing the quantum computation [1, 2, 3, 4]. The decoherence is caused by interaction between the quantum computer and its environment. The interaction lets the state of the computer

*On leave from Canon Inc., 5-1, Morinosato-Wakamiya, Atsugi-shi, Kanagawa, 243-0193, Japan.

become correlated with the state of the environment. Consequently, some of information of the quantum computer leaks into the environment. This process causes errors in the state of the quantum computer, and as a result, the probability that the quantum algorithm gives the right answer decreases. To overcome this problem, quantum error-correcting codes are proposed [5, 6, 7].

Not only for practical purposes but also for theoretical interests, an important question is how robust the quantum algorithm is against this disturbance. If we know the upper bound of the error rate that allows the quantum computer to obtain a solution with a certain probability or more, this bound is useful for us to design quantum gates.

Grover's algorithm is considered to be an efficient amplitude-amplification process for quantum states. Thus it is often called a search algorithm [8, 9]. By applying the same unitary transformation to the state in iteration and gradually amplifying an amplitude of one basis vector that an oracle indicates, Grover's algorithm picks it up from a uniform superposition of $2^n$ basis vectors with a certain probability in $O(2^{n/2})$ steps. In view of computational time (the number of queries for the oracle), the efficiency of Grover's algorithm is proved to be optimal [10].

In Ref. [11], we study decoherence in Grover's algorithm with a perturbative method. We consider the following simple model. First, we assume that we search $|0...0\rangle$ from the uniform superposition of $2^n$ logical basis vectors $\{|x\rangle : x \in \{0,1\}^n\}$ by Grover's algorithm. This assumption simplifies the iterative transformation. Second, we assume that each qubit of the register interacts with the environment independently and suffers a phase damping, which causes a phase flip error ($\sigma_z$ error) with probability $p$ and does nothing with probability $(1-p)$ to the qubit. In this model, we expand an $n$-qubit density operator to which Grover's iterative operation is applied $M$ times in powers of $2Mnp$. Then, we take the large-$n$ limit, so that we can simplify each order term of the expansion of the density operator and we obtain its asymptotic form.

In this large-$n$ limit, we assume $p$ is small enough, so that $2Mnp$ can take any real positive value or zero. We regard $x \equiv 2Mnp(\geq 0)$ as a perturbative parameter. We can interpret $x = 2Mnp$ as the expected number of phase flip errors ($\sigma_z$ errors) that occur during the running time of computation. In Ref. [11], we give a formula for deriving an asymptotic form of an arbitrary order term of the perturbative expansion. However, this formula includes a complicated multiple integral and the number of terms in its integrand increases exponentially. Because of these difficulties, we obtain explicit asymptotic forms only up to the fifth-order term.

In this paper, using recurrence relations between terms of the perturbative expansion, we develop a method for computing higher order terms efficiently. By this method, we derive an explicit form of the density matrix of the disturbed quantum computer up to the 39th-order term with the help of a computer algebra system. (In actual fact, we use *Mathematica* for this derivation.) Because we consider the higher order perturbation, we can greatly extend the range of the perturbative parameter that provides a reliable analysis, compared with our previous work in Ref. [11]. Calculating the matrix element up to the 39th-order term numerically from the form obtained by the computer algebra system, we derive the maximum value of the perturbative parameter $x$ at which the algorithm finds a correct item with a given threshold of probability $P_{\rm th}$ or more. (We refer to this maximum value of $x$ as $x_{\rm c}$, a critical point of $x$.)

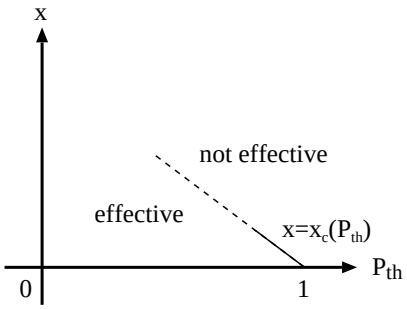


Figure 1: A schematic representation of $x_{\rm c}$ as a function of $P_{\rm th}$. $P_{\rm th}$ is a threshold of probability. $x$ represents both the perturbative parameter and the expected number of errors during the running time of computation. $x_{\rm c}$ is a critical point of $x$. Both $P_{\rm th}$ and $x$ are dimensionless. We can easily obtain $x_{\rm c} = 0$ for $P_{\rm th} = 1$. This fact is included in the above schematic graph. The above graph represents a phase diagram that consists of two domains. One domain is where the quantum algorithm is effective and the other domain is where it is not effective.

Grover's algorithm can find the correct item by less than $(\pi/4)\sqrt{2^n}$ steps with given probability $P_{\rm th}$ or more under no decoherence ($p = 0$). When we fix $P_{\rm th}$, the number of iterations that we need increases as the decoherence becomes stronger ($p$ becomes larger). Finally we never detect the correct item with $P_{\rm th}$ or more for $p > p_{\rm c}$. Thus, we can think $p_{\rm c}$ to be a critical point for $P_{\rm th}$. ($p_{\rm c}$ depends on $P_{\rm th}$.) However, we actually obtain $x_{\rm c} = x_{\rm c}(P_{\rm th})$ for the perturbative parameter $x = 2Mnp$ instead of $p_{\rm c} = p_{\rm c}(P_{\rm th})$. From the relation $x_{\rm c} = x_{\rm c}(P_{\rm th})$, we can draw a phase diagram as shown in Fig. 1. The diagram consists of two domains. One is where the quantum algorithm is effective and the other is where it is not effective.

Figures 2 and 3 represent a curve of $x_{\rm c} = x_{\rm c}(P_{\rm th})$ obtained by repeating the numerical calculation of $x_{\rm c}$ for many points of $P_{\rm th}$. In Fig. 2, we use a linear scale on both horizontal and vertical axes. We prove later that a tangent of the curve $x = x_{\rm c}(P_{\rm th})$ at $P_{\rm th} = 1$ is given by $x = (8/5)(1 - P_{\rm th})$. In Fig. 3, we use log and linear scales on the horizontal and vertical axes, respectively. We observe $x_{\rm c} > -(8/5)\log_e P_{\rm th}$ near $P_{\rm th} = 0$ from this figure.

Here, we mention that we can investigate our model by Monte Carlo simulations, as well. In fact, we compare results obtained by our perturbative method with results obtained by Monte Carlo simulations in Figs. 5 and 6 in Sec. 4, and we confirm that they are consistent. From these analyses, we conclude that our perturbative method is valid in a certain range of the perturbative parameter.

However, the Monte Carlo simulation method has some difficulties for investigating our model. First, the execution time of computation increases exponentially in $n$ (the number of qubits). We have to always come up against this problem when we simulate a process of a quantum computer with a classical computer. Second, the Monte Carlo simulation method is not suitable for obtaining a variation of a physical quantity as a function of some parameters, because we carry out each simulation with fixing parameters such as the error rate $p$ and the threshold of probability $P_{\rm th}$. Thus we prefer our perturbative method to the Monte Carlo simulation method for computing $x_{\rm c}$ (the critical point of $x$)

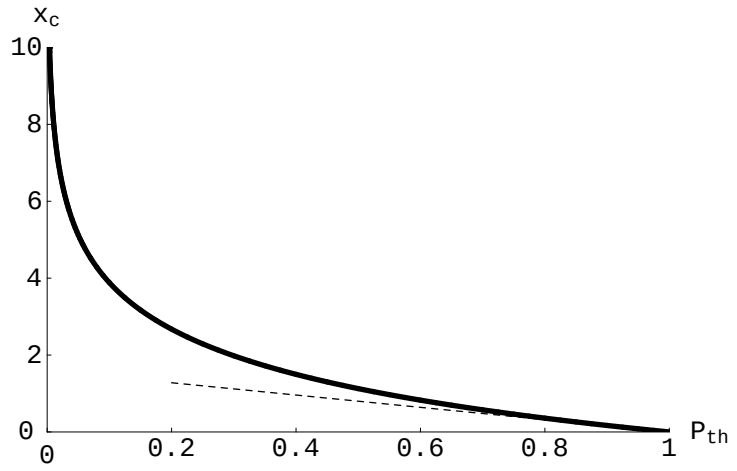


Figure 2: $x_{\rm c}$ as a function of $P_{\rm th}$. [A thick solid curve represents $x = x_{\rm c}(P_{\rm th})$.] $P_{\rm th}$ is a threshold of probability. $x_{\rm c}$ is a critical point of $x$ (the perturbative parameter). We use a linear scale on both horizontal and vertical axes. The data are obtained by repeating numerical calculation of $x_{\rm c}$ for many points of $P_{\rm th}$. Because $x = x_{\rm c}(P_{\rm th})$ shows a sharp divergence at $P_{\rm th} = 0$, we start calculation of $x_{\rm c}$ from $P_{\rm th} = 1$. While we are going from $P_{\rm th} = 1$ toward $P_{\rm th} = 0$, we make a finite difference of $P_{\rm th}$ smaller gradually. (We put $\Delta P_{\rm th} = 5.0 \times 10^{-4}$ around $P_{\rm th} = 1$ and $\Delta P_{\rm th} = 5.0 \times 10^{-7}$ around $P_{\rm th} = 3.7 \times 10^{-3}$.) A thin dashed line represents a tangent of $x = x_{\rm c}(P_{\rm th})$ at $P_{\rm th} = 1$.

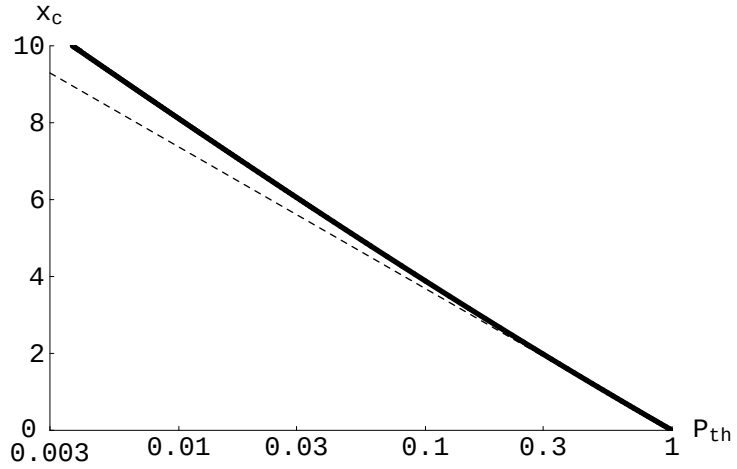


Figure 3: $x_{\rm c}$ as a function of $P_{\rm th}$. [A thick solid curve represents $x = x_{\rm c}(P_{\rm th})$.] We use log and linear scales on the horizontal and vertical axes, respectively. In this figure, we use the same data of $x = x_{\rm c}(P_{\rm th})$ as in Fig. 2. A thin dashed line represents $x = -(8/5)\log_e P_{\rm th}$. We observe $x_{\rm c} > -(8/5)\log_e P_{\rm th}$ near $P_{\rm th} = 0$.

that is obtained by evaluating the probability of detecting a correct answer as a function of $x$ and $P_{\rm th}$.

A related result is obtained in the study of the accuracy of quantum gates by Bernstein and Vazirani [12], and Preskill [13]. They consider a quantum circuit where each quantum gate has a constant error because of inaccuracy. Thus, it is an error of a unitary transformation and it never causes dissipation of information from the quantum computer to its environment. They estimate inaccuracy $\epsilon$ for which the quantum algorithm is effective under the fixed number of time steps $T$, and obtain $2T\epsilon < 1 - P_{\rm th}$, where $0 \leq \epsilon \ll 1$. If we regard $p/2$ as inaccuracy $\epsilon$ and $2Mn$ as the number of whole steps in the algorithm $T$, it is similar to our observation that $x_{\rm c} = 2Mnp \simeq (8/5)(1 - P_{\rm th})$ near $P_{\rm th} = 1$, except for a factor.

Barenco *et al.* study the approximate quantum Fourier transformation (AQFT) and its decoherence [14]. Although their motivation is slightly different from Refs. [12, 13], we can think their model to be the quantum Fourier transformation (QFT) with inaccurate gates. They confirm that AQFT can give a performance that is not much worse than the QFT.

This article is organized as follows. In Sec. 2, we describe our model and perturbation theory defined in our previous work [11]. In Sec. 3, we give recurrence relations between terms of the perturbative expansion. We develop a method for calculating higher order perturbation efficiently with these relations. In Sec. 4, we carry out numerical calculations of the matrix element of the density operator by the efficient method obtained in Sec. 3. Moreover, we investigate the critical point $x_{\rm c}$ and obtain the phase diagram shown in Figs. 2 and 3. In Sec. 5, we give brief discussions. In Appendix A, we give a proof of an equation which appears in Sec. 3.

# 2 Model and perturbation theory

In this section, we first describe a model that we analyze. It is a quantum process of Grover's algorithm under a phase damping at every iteration. Second, we formulate a perturbation theory for this model.

## 2.1 Model

First of all, we give a brief review of Grover's algorithm [8]. Starting from the $n$-qubit uniform superposition of logical basis vectors,

$$W|0...0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \qquad \text{for } n \geq 2, \tag{1}$$

Grover's algorithm gradually amplifies the amplitude of a certain basis vector $|x_0\rangle$ that a quantum oracle indicates, where $x_0 \in \{0,1\}^n$. The operator $W$ in Eq. (1) is an $n$-fold tensor product of a one-qubit unitary transformation and given by $W = H^{\otimes n}$. The operator $H$ is called Hadamard transformation and represented by the following matrix,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2}$$

where we use the orthonormal basis $\{|0\rangle, |1\rangle\}$ for this matrix representation. The quantum oracle can be regarded as a black box and actually it is a quantum gate that shifts phases of logical basis vectors as

$$R_{x_0}: \quad \begin{cases} |x_0\rangle & \rightarrow & -|x_0\rangle \\ |x\rangle & \rightarrow & |x\rangle \qquad \text{for } x \neq x_0 \end{cases}, \tag{3}$$

where $x_0, x \in \{0,1\}^n$. [We note that all operators (quantum gates) in Grover's algorithm are unitary. Thus, $H^\dagger = H^{-1}$, $W^\dagger = W^{-1}$, $R_{x_0}^\dagger = R_{x_0}^{-1}$, and so on.]

To let probability of observing $|x_0\rangle$ be greater than a certain value (1/2, for example), we repeat the following procedure $O(\sqrt{2^n})$ times:

1. Apply $R_{x_0}$ to the $n$-qubit state.
2. Apply $D = WR_0W$ to the $n$-qubit state.

$R_0$ is a selective phase-shift operator, which multiplies a factor $(-1)$ to $|0...0\rangle$ and does nothing to the other basis vectors, as defined in Eq. (3). $D$ is called the inversion-about-average operation.

From now on, we assume that we amplify an amplitude of $|0...0\rangle$. From this assumption, we can write an operation iterated in the algorithm as

$$DR_0 = (WR_0W)R_0. \tag{4}$$

After repeating this operation $M$ times from the initial state $W|0\rangle (= W|0...0\rangle)$, we obtain the state $(WR_0)^{2M}W|0\rangle$. (We often write $|0\rangle$ as an abbreviation of the $n$-qubit state $|0...0\rangle$ for a simple notation.)

Next, we think about the decoherence. In this paper, we consider the following one-qubit phase damping [15, 16]:

$$\rho \rightarrow \rho' = p\sigma_z\rho\sigma_z + (1-p)\rho \qquad \text{for } 0 \leq p \leq 1, \tag{5}$$

where $\rho$ is an arbitrary one-qubit density operator. $\sigma_z$ is one of the Pauli matrices and given by

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{6}$$

where we use the orthonormal basis $\{|0\rangle, |1\rangle\}$ for this matrix representation. For simplicity, we assume that the phase damping of Eq. (5) occurs in each qubit of the register independently before every $R_0$ operation during the algorithm. This implies that each qubit interacts with its own environment independently.

Here, we add some notes. First, because $R_0 \in U(2^n)$ is applied to all $n$ qubits and $H \in U(2)$ is applied to only one qubit, we can imagine that the realization of $R_0$ is more difficult than that of $W = H^{\otimes n}$. Hence, we assume that the phase damping occurs only before $R_0$. Second, although we assume a very simple decoherence defined in Eq. (5), we can think of other complicated disturbances. For example, we can consider decoherence caused by an interaction between the environment and two qubits and it may occur with a probability of $O(p^2)$. In this paper, we do not assume such complicated disturbances.

## 2.2 Perturbation theory

Let $\rho^{(M)}$ be the density operator obtained by applying Grover's iteration $M$ times to the $n$-qubit initial state $W|0\rangle$. The decoherence defined in Eq. (5) occurs $2Mn$ times in $\rho^{(M)}$. We can expand $\rho^{(M)}$ in powers of $p$ and $(1-p)$ as follows:

$$\begin{aligned}\rho^{(M)} &= (1-p)^{2Mn}T_0^{(M)} + (1-p)^{2Mn-1}pT_1^{(M)} + ... \\ &= \sum_{k=0}^{2Mn}(1-p)^{2Mn-k}p^k T_k^{(M)}, \end{aligned} \tag{7}$$

where $\{T_k^{(M)}\}$ are given by

$$T_0^{(M)} = (WR_0)^{2M}W|0\rangle\langle 0|W(R_0W)^{2M}, \tag{8}$$

$$T_1^{(M)} = \sum_{i=1}^{n}\sum_{l=0}^{2M-1}(WR_0)^{2M-l}\sigma_z^{(i)}(WR_0)^l W|0\rangle\langle 0|W(R_0W)^l\sigma_z^{(i)}(R_0W)^{2M-l}, \tag{9}$$

$$\begin{aligned}T_2^{(M)} &= \sum_{i=1}^{n}\sum_{\substack{j=1\\ i<j}}^{n}\sum_{l=0}^{2M-1}(WR_0)^{2M-l}\sigma_z^{(i)}\sigma_z^{(j)}(WR_0)^l W|0\rangle\langle \text{H.c.}| \\ &\quad + \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{l=0}^{2M-1}\sum_{m=1}^{2M-l-1}(WR_0)^{2M-l-m}\sigma_z^{(i)}(WR_0)^m\sigma_z^{(j)}(WR_0)^l W|0\rangle \\ &\qquad \times\langle \text{H.c.}|, \end{aligned} \tag{10}$$

and so on, $\sigma_z^{(i)}$ represents the operator applied to the $i$th qubit for $1 \le i \le n$, and $\langle$H.c.$|$ represents a Hermitian conjugation of the ket vector on its left side. (Here, we note $W^\dagger = W$, $R_0^\dagger = R_0$, and $\sigma_z^{(i)\dagger} = \sigma_z^{(i)}$.) We can regard $T_k^{(M)}$ as a density operator whose trace is not normalized. It represents the sum of states where $k$ errors occur during the iteration of $M$ operations.

On the other hand, from Eq. (7), we can expand $\rho^{(M)}$ in powers of $p$ as follows:

$$\begin{aligned}\rho^{(M)} &= \rho_0^{(M)} + 2Mnp\rho_1^{(M)} + \frac{1}{2}(2Mn)(2Mn-1)p^2\rho_2^{(M)} + ... \\ &= \sum_{k=0}^{2Mn}\binom{2Mn}{k}p^k\rho_k^{(M)}, \end{aligned} \tag{11}$$

where

$$\begin{aligned}\rho_0^{(M)} &= T_0^{(M)}, \\ \rho_1^{(M)} &= -T_0^{(M)} + \frac{T_1^{(M)}}{2Mn}, \\ \rho_k^{(M)} &= (-1)^k\sum_{j=0}^{k}(-1)^j\binom{2Mn}{j}^{-1}\binom{k}{j}T_j^{(M)} \qquad \text{for } k = 0, 1, ..., 2Mn. \end{aligned} \tag{12}$$

Here, let us take the limit of an infinite number of qubits (the large-$n$ limit). We assume that we can take very small $p$, so that $2Mnp$ can be an arbitrary real positive value or

zero. If $2Mnp$ is small enough, we can consider $x \equiv 2Mnp (\geq 0)$ to be a perturbative parameter and the series of Eq. (11) to be a perturbative expansion.

Under this limit, we derive an asymptotic form of $\langle 0|\rho^{(M)}|0\rangle$. In the actual derivation, we take the limit of $n \to \infty$ with holding $x = 2Mnp$ finite. $\langle 0|\rho^{(M)}|0\rangle$ is a probability that the quantum computer finds a correct item after $M$ operations. Because we divide $T_j^{(M)}$ by $(Mn)^j$ as in Eq. (12), an expectation value of $\rho_k^{(M)}$ can converge to a finite value in the limit $n \to \infty$ for $k = 0, 1, ..., 2Mn$.

With these preparations, we will investigate the following physical quantities. Let $P_{\rm th}$ be a threshold of probability for $0 < P_{\rm th} \leq 1$, so that if the quantum computer finds a correct item (in our model, it is $|0\rangle$) with probability $P_{\rm th}$ or more, we regard it effective, and otherwise we do not consider it effective. Then, we consider the least number of the operations that we need to repeat for amplifying the probability of observing $|0\rangle$ to $P_{\rm th}$ or more for a given $p$. We refer to it as $M_{\rm th}(p, P_{\rm th})$. [$M_{\rm th}(p, P_{\rm th})$ is the least number of $M$ that satisfies $\langle 0|\rho^{(M)}|0\rangle = P_{\rm th}$ for a given $p$.] As $p$ becomes larger with fixing $P_{\rm th}$, we can expect that $M_{\rm th}(p, P_{\rm th})$ increases monotonically. In the end, we never observe $|0\rangle$ at least with a probability $P_{\rm th}$ for a certain $p_{\rm c}$ or more. (Hence, $p_{\rm c}$ depends on $P_{\rm th}$.) Regarding $P_{\rm th}$ as a threshold for whether the quantum computer is effective or not, we can consider $p_{\rm c}$ to be a critical point.

In our perturbation theory, we calculate physical quantities using the dimensionless perturbative parameter $x = 2Mnp$. Thus, we take $M$ and $x$ for independent variables. (In our original model defined in Sec. 2.1, we take $M$ and $p$ for independent variables.) We can define as well $\tilde{M}_{\rm th}(x, P_{\rm th})$ that represents the least number of the operations iterated for amplifying the probability of $|0\rangle$ to $P_{\rm th}$ for given $x$. Furthermore, we also obtain $x_{\rm c}$ or more for which we can never detect $|0\rangle$ at least with probability $P_{\rm th}$.

Next, we evaluate $\langle 0|\rho^{(M)}|0\rangle$. First, from simple calculation, we obtain the unperturbed matrix element,

$$\begin{aligned} \langle 0|\rho^{(M)}|0\rangle_{p=0} &= \langle 0|T_0^{(M)}|0\rangle \\ &= \sin^2[(2M+1)\theta], \end{aligned} \tag{13}$$

where

$$\sin\theta = \frac{1}{\sqrt{2^n}}, \qquad \cos\theta = \sqrt{\frac{2^n - 1}{2^n}}. \tag{14}$$

(This parameter $\theta$ is introduced by Boyer *et al.* [9].) From Eq. (13), we notice the following facts. If there is no decoherence ($p = 0$), we can amplify the probability of observing $|0\rangle$ to unity. Taking large (but finite) $n$, we obtain $\sin\theta \simeq \theta$ and $\theta \simeq 1/\sqrt{2^n}$, and we can observe $|0\rangle$ with unit probability after repeating Grover's operation $M_{\rm max} \simeq (\pi/4)\sqrt{2^n}$ times.

To describe the asymptotic forms of matrix elements, we introduce the following notation. Because $\langle 0|T_0^{(M)}|0\rangle$ is a periodic function of $M$ and its period is about $\pi\sqrt{2^n}$ under the large-$n$ limit, it is convenient for us to define a new variable $\Theta = \lim_{n\to\infty} M\theta$ (radian). Here, we give a formula for the asymptotic form of the $k$th order of the matrix element under $n \to \infty$ for $k = 1, 2, ....$ (The derivation of this formula is given in Secs. 4–7 and Appendix A of Ref. [11].) Preparing an $k$-digit binary string $\alpha = (\alpha_1, ..., \alpha_k) \in \{0, 1\}^k$,

we define the following $2^k$ terms:

$$
\begin{aligned}
&|\tilde{\mathcal{T}}_{\alpha_1,...,\alpha_k}(\phi_1,...,\phi_k)|^2 \\
&= [\begin{Bmatrix}\sin\\ \cos\end{Bmatrix}_{\alpha_1}(2\phi_1)\begin{Bmatrix}\cos\\ \sin\end{Bmatrix}_{\alpha_2}(2\phi_2)...\begin{Bmatrix}\cos\\ \sin\end{Bmatrix}_{\alpha_k}(2\phi_k)\begin{Bmatrix}\cos\\ \sin\end{Bmatrix}_{\oplus_{s=1}^k\alpha_s}(2[\Theta-\sum_{s=1}^k\phi_s])]^2 \\
&\qquad \text{for } k=1,2,...,
\end{aligned}
\tag{15}
$$

where

$$
\begin{Bmatrix} f\\ g\end{Bmatrix}_\alpha(x) = \begin{cases} f(x) & \text{for } \alpha=0 \\ g(x) & \text{for } \alpha=1 \end{cases}, \tag{16}
$$

and $\oplus$ denotes the addition modulo 2. We notice that the function of $\phi_1$ and the other functions of $\phi_2$,..., $\phi_k$, $\Theta-\sum_{s=1}^k\phi_s$ are different (sine and cosine functions are put in reverse). These terms are integrated as

$$
\begin{aligned}
&\lim_{n\to\infty}\frac{\langle 0|T_k^{(M)}|0\rangle}{(Mn)^k} \\
&= \frac{1}{\Theta^k}\int_0^\Theta d\phi_1\int_0^{\Theta-\phi_1}d\phi_2...\int_0^{\Theta-\phi_1-...-\phi_{k-1}}d\phi_k \\
&\qquad \times\sum_{(\alpha_1,...,\alpha_k)\in\{0,1\}^k}|\tilde{\mathcal{T}}_{\alpha_1,...,\alpha_k}(\phi_1,...,\phi_k)|^2.
\end{aligned}
\tag{17}
$$

We can obtain the matrix elements as follows. From Eq. (13), we obtain

$$
\lim_{n\to\infty}\langle 0|T_0^{(M)}|0\rangle = \sin^2 2\Theta. \tag{18}
$$

From Eqs. (15) and (17), we obtain

$$
\begin{aligned}
\lim_{n\to\infty}\frac{\langle 0|T_1^{(M)}|0\rangle}{Mn} &= \frac{1}{\Theta}\int_0^\Theta d\phi\{[\sin 2\phi\cos 2(\Theta-\phi)]^2+[\cos 2\phi\sin 2(\Theta-\phi)]^2\} \\
&= \frac{1}{2}-\frac{1}{4}\cos 4\Theta-\frac{1}{16\Theta}\sin 4\Theta,
\end{aligned}
\tag{19}
$$

$$
\begin{aligned}
\lim_{n\to\infty}\frac{\langle 0|T_2^{(M)}|0\rangle}{(Mn)^2} &= \frac{1}{\Theta^2}\int_0^\Theta d\phi\int_0^{\Theta-\phi}d\varphi \\
&\qquad \times\{[\sin 2\phi\cos 2\varphi\cos 2(\Theta-\phi-\varphi)]^2 \\
&\qquad +[\cos 2\phi\cos 2\varphi\sin 2(\Theta-\phi-\varphi)]^2 \\
&\qquad +[\sin 2\phi\sin 2\varphi\sin 2(\Theta-\phi-\varphi)]^2 \\
&\qquad +[\cos 2\phi\sin 2\varphi\cos 2(\Theta-\phi-\varphi)]^2\} \\
&= \frac{1}{4}-\frac{1}{16}\cos 4\Theta-\frac{3}{64\Theta}\sin 4\Theta,
\end{aligned}
\tag{20}
$$

and so on.

The asymptotic form of the perturbative expansion of the whole density matrix is given by

$$\begin{aligned}\langle P\rangle(\Theta,x) &= \lim_{n\to\infty}\langle 0|\rho^{(M)}|0\rangle \\ &= C_0(\Theta)+C_1(\Theta)x+\frac{1}{2}C_2(\Theta)x^2+... \\ &= \sum_{k=0}^{\infty}C_k(\Theta)\frac{1}{k!}x^k, \end{aligned} \tag{21}$$

where

$$\begin{aligned} C_0(\Theta) &= F_0(\Theta), \\ C_1(\Theta) &= -F_0(\Theta)+\frac{1}{2}F_1(\Theta), \\ C_k(\Theta) &= (-1)^k\sum_{j=0}^{k}(-\frac{1}{2})^j\frac{k!}{(k-j)!}F_j(\Theta) \qquad \text{for } k=0,1,..., \end{aligned} \tag{22}$$

and

$$F_k(\Theta)=\lim_{n\to\infty}\frac{\langle 0|T_k^{(M)}|0\rangle}{(Mn)^k} \qquad \text{for } k=0,1,.... \tag{23}$$

In Eq. (21), the $k$th-order term is divided by $k!$, so that we can expect the series $\langle P\rangle(\Theta,x)$ to converge to a finite value for large $x$.

# 3 Recurrence relations between order terms

In this section, we obtain recurrence relations between order terms of the perturbative series. Using this result, we develop a method for computing higher order terms efficiently.

When we compute $\lim_{n\to\infty}\langle 0|T_k^{(M)}|0\rangle/(Mn)^k$ for large $k$ from Eqs. (15) and (17), we notice the following difficulties:

1. Equation (17) includes an $k$th-order integral.
2. Equation (17) includes $2^k$ terms being integrated.

Even if we use a computer algebra system, these troubles are serious. (In Ref. [11], we obtain $\lim_{n\to\infty}\langle 0|T_k^{(M)}|0\rangle/(Mn)^k$ only up to $k=5$.)

To develop an efficient derivation of higher order terms, we pay attention to the following relations:

$$F_k(\Theta)=\lim_{n\to\infty}\frac{\langle 0|T_k^{(M)}|0\rangle}{(Mn)^k}=\frac{f_k(\Theta)}{\Theta^k} \qquad \text{for } k=0,1,..., \tag{24}$$

where

$$f_0(\Theta) = \sin^2 2\Theta, \tag{25}$$

$$g_0(\Theta) = \cos^2 2\Theta, \tag{26}$$

$$f_k(\Theta) = \int_0^\Theta d\phi [f_{k-1}(\Theta-\phi)\cos^2 2\phi + g_{k-1}(\Theta-\phi)\sin^2 2\phi], \tag{27}$$

$$g_k(\Theta) = \int_0^\Theta d\phi [g_{k-1}(\Theta-\phi)\cos^2 2\phi + f_{k-1}(\Theta-\phi)\sin^2 2\phi] \tag{28}$$

$$\text{for } k = 1, 2, ....$$

We can prove the above relations from Eqs. (15) and (17). Both Eqs. (27) and (28) contain only first-order integrals. Moreover, each of them contains only two terms being integrated. Thus, we can compute $F_0(\Theta)$, $F_1(\Theta)$, ... in that order efficiently from Eqs. (24), (25), (26), (27), and (28) using a computer algebra system. (In actual fact, we use *Mathematica* for this derivation.) Eqs. (27) and (28) constitute a pair of recurrence formulas.

Here, we note some properties of $F_k(\Theta)$. First, $f_k(\Theta)$ and $g_k(\Theta)$ are analytic at any $\Theta$ for $k = 0, 1, ....$ In other words, $f_k(\Theta)$ and $g_k(\Theta)$ have Taylor expansions about any $\Theta_0$ which converge to $f_k(\Theta)$ and $g_k(\Theta)$ in some neighborhood of $\Theta_0$ for $k = 0, 1, ...,$ respectively. We can prove these facts by mathematical induction as follows. To begin with, both $f_0(\Theta)$ and $g_0(\Theta)$ are analytic at any $\Theta$ from Eqs. (25) and (26). Next, we assume that $f_k(\Theta)$ and $g_k(\Theta)$ are analytic at any $\Theta$ for some $k \in \{0, 1, ...\}$. Then, $f_{k+1}(\Theta)$ and $g_{k+1}(\Theta)$ are analytic at any $\Theta$ because they are integrals of functions made of the sine and cosine functions, $f_k(\Theta)$, and $g_k(\Theta)$, as shown in Eqs. (27) and (28). Thus, by mathematical induction, we conclude that $f_k(\Theta)$ and $g_k(\Theta)$ are analytic functions for $k = 0, 1, ....$

From Eq. (24), we can obtain $F_k(\Theta)$ by dividing $f_k(\Theta)$ by $\Theta^k$ for $k = 0, 1, ....$ Thus, it is possible that $F_k(\Theta)$ diverges by marching off to infinity near $\Theta = 0$. However, in fact we can show

$$F_k(\Theta) = \frac{f_k(\Theta)}{\Theta^k} = \text{Const.}\Theta^2 + O(\Theta^4) \qquad \text{for } k = 0, 1, ..., \tag{29}$$

where Const. denotes some constant. (We prove Eq. (29) in Appendix A.)

# 4 Numerical calculations

In this section, we carry out numerical calculations of $\langle P\rangle(\Theta, x)$ defined in Eq. (21) using recurrence relations Eqs. (27) and (28). Moreover, we investigate the critical point $x_{\rm c}$, over which the quantum algorithm becomes ineffective for the threshold probability $P_{\rm th}$.

First of all, we need to derive an algebraic representation of $\langle P\rangle(\Theta, x)$. We compute an explicit form of $\langle P\rangle(\Theta, x)$ as follows. First, using recurrence relations Eqs. (27) and (28), we derive $f_k(\Theta)$ and $g_k(\Theta)$. Second, using Eq. (24), we derive $F_k(\Theta)$ from $f_k(\Theta)$. Next, using Eq. (22), we derive $C_k(\Theta)$ from $F_k(\Theta)$. Finally, using Eq. (21), we derive $\langle P\rangle(\Theta, x)$ from $C_k(\Theta)$, which is the $k$th-order term of the perturbative expansion.

In Ref. [11], we obtain an explicit form of the matrix element only up to the fifth-order perturbation [that is, $F_5(\Theta)$] because we compute $F_k(\Theta)$ from Eq. (17) directly. However, in this paper, we succeed in deriving an explicit form of the matrix element up to the 39th-order perturbation [that is, $F_{39}(\Theta)$] with the help of the computer algebra system thanks to the recurrence relations Eqs. (27) and (28). [We do not write down the explicit

forms of $F_3(\Theta)$, ..., $F_{39}(\Theta)$ here except for $F_5(\Theta)$, because they are very complicated.] By the method explained above, we derive the algebraic form of $\langle P\rangle(\Theta, x)$ up to the 39th-order perturbation.

However, this explicit form of $\langle P\rangle(\Theta, x)$ is not suitable for numerical calculation. The reason is as follows. Let us consider $F_5(\Theta)$ for example. The explicit form of $F_5(\Theta)$ is given by

$$\begin{aligned} F_5(\Theta) &= \frac{1}{240} + \frac{45 + 720\Theta^2 - 256\Theta^4}{1\ 966\ 080\Theta^4}\cos 4\Theta \\ &\quad - \frac{3 + 32\Theta^2 + 256\Theta^4}{524\ 288\Theta^5}\sin 4\Theta. \end{aligned} \tag{30}$$

It is very difficult to evaluate the value of $F_5(\Theta)$ near $\Theta = 0$ from Eq. (30) directly. If we take the limit $\Theta \to 0$ in the second term of Eq. (30), we obtain

$$\lim_{\Theta\to 0} \frac{45 + 720\Theta^2 - 256\Theta^4}{1\ 966\ 080\Theta^4}\cos 4\Theta = +\infty. \tag{31}$$

However, taking the limit $\Theta \to 0$ in the third term of Eq. (30), we obtain

$$\begin{aligned} & \lim_{\Theta\to 0}(-\frac{3 + 32\Theta^2 + 256\Theta^4}{524\ 288\Theta^5})\sin 4\Theta \\ = & -\lim_{\Theta\to 0}(\frac{3 + 32\Theta^2 + 256\Theta^4}{131\ 072\Theta^4})\frac{\sin 4\Theta}{4\Theta} \\ = & -\infty. \end{aligned} \tag{32}$$

As explained above, to evaluate the value of $F_5(\Theta)$ near $\Theta = 0$ from Eq. (30) directly, we have to subtract one huge value from another huge value. Thus, if we carry out this operation by computer, an underflow error occurs and we cannot predict a result of the numerical calculation at all. [We show that $F_k(\Theta)$ is analytic at $\Theta = 0$ and $\lim_{\Theta\to 0} F_k(\Theta) = 0$ for $k = 0, 1, ...$ in Eq. (29). However, it is difficult to calculate $F_5(\Theta)$ numerically from Eq. (30).]

In fact, when $\Theta = 1.0\times 10^{-7}$, the second term of Eq. (30) is equal to $2.28881\times 10^{23}$ and the third term of Eq. (30) is equal to $-2.28881 \times 10^{23}$ with assuming that the computer supports only six significant figures. Hence, the sum of the second term and the third term in Eq. (30) is equal to zero, and only the first term of Eq. (30), 1/240, contributes to $F_5(\Theta)$ for $\Theta = 1.0 \times 10^{-7}$. However, this numerical calculation is meaningless. We can find such an underflow error in almost all the higher order terms, $F_3(\Theta)$, $F_4(\Theta)$, $F_5(\Theta)$, ....

To avoid this trouble, we carry out the following procedure. We expand the explicit form of $C_k(\Theta)$ in powers of $\Theta$ up to the 40th-order term and define $\bar{C}_k(\Theta)$ as the finite power series obtained in the variable $\Theta$ for $k = 0, 1, ..., 39$. [$C_k(\Theta)$ is originally an analytic function and it has a Taylor expansion about $\Theta = 0$.] We substitute these $\{\bar{C}_k(\Theta) : k = 0, 1, ..., 39\}$ for Eq. (21) and obtain

$$\langle \bar{P}\rangle(\Theta, x) = \sum_{k=0}^{39} \bar{C}_k(\Theta)\frac{1}{k!}x^k. \tag{33}$$

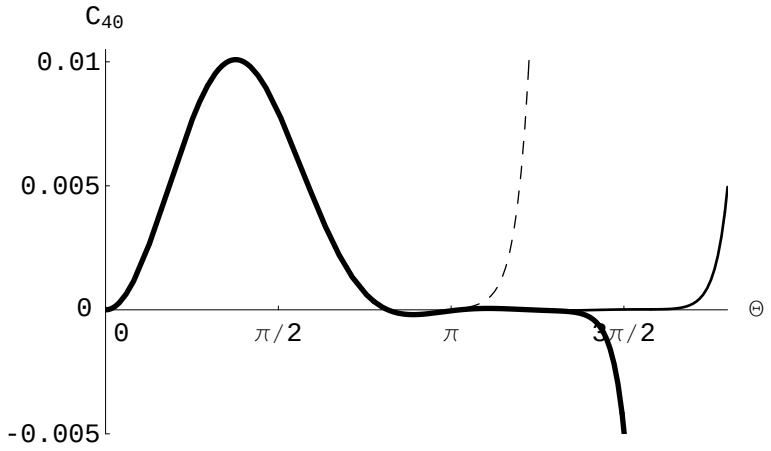


Figure 4: 30th, 40th, and 50th-order polynomials, which we obtain as parts of Taylor series of $C_{40}(\Theta)$, as functions of $\Theta$ for $0 \leq \Theta \leq (9/5)\pi$. A dashed line, a thick solid line, and a thin solid line represent the 30th, 40th, and 50th-order polynomials, respectively.

We use this $\langle \bar{P} \rangle(\Theta, x)$ for numerical calculation. [$\langle \bar{P} \rangle(\Theta, x)$ is a polynomial, whose highest power in $\Theta$ is equal to 40 and whose highest power in $x$ is equal to 39.]

Here, we make some comments on our approximation method for $C_k(\Theta)$. In this paper, we use a polynomial of high degree for approximating $C_k(\Theta)$. The reasons for this choice are as follows: (1) to obtain the Taylor series of $C_k(\Theta)$ is easy, and (2) because we can calculate integrals and derivatives of polynomials with ease, $\bar{C}_k(\Theta)$ is suitable for applying Newton's method. (We use Newton's method for calculating $x_{\rm c}$ later.) However, approximation with a polynomial of high degree sometimes causes oscillations, and consequently errors of numerical calculation. Padé approximant method is effective in the treatment of this problem. However, we do not use this method here, because we have to carry out tough calculations for deriving the Padé approximants of $C_k(\Theta)$.

We use a 40th-order polynomial for approximating $C_k(\Theta)$ in this paper. Figure 4 shows 30th, 40th, and 50th-order polynomials, which we obtain as parts of Taylor series of $C_{40}(\Theta)$, as functions of $\Theta$ for $0 \leq \Theta \leq (9/5)\pi$. A dashed line, a thick solid line, and a thin solid line represent the 30th, 40th, and 50th-order polynomials, respectively. From Fig. 4, we find that the 30th, 40th, and 50th-order polynomials start to diverge near $\Theta = 3.4$, 4.3, and 5.3(radian), respectively. From this observation, we think the approximation of $C_{40}(\Theta)$ with the 40th-order polynomial, that is $\bar{C}_{40}(\Theta)$, to be valid in the range of $0 \leq \Theta \leq \pi$. [Strictly speaking, this is not a rigorous proof but evidence that the polynomial expansion up to the 40th-order term is sufficient for approximating $C_k(\Theta)$ for $k = 0, 1, ..., 39$ in the range of $0 \leq \Theta \leq \pi$.]

To investigate the range of $x$ where our perturbative approach is valid, we need to estimate the 40th-order perturbation. From numerical calculation, we obtain

$$0 \leq |\frac{1}{40!}\bar{C}_{40}(\Theta)| \leq 1.24 \times 10^{-50} \tag{34}$$

for $0 \leq \Theta \leq \pi$. (From now on, we limit $\Theta$ to $0 \leq \Theta \leq \pi$ for our analysis, because the

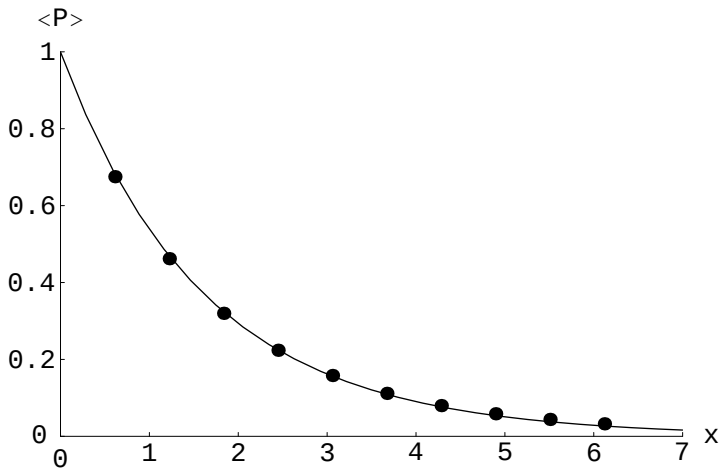


Figure 5: $\langle P\rangle(\Theta, x)$ as a function of $x$ with fixing $\Theta = \Theta_{\max}$, where $\Theta_{\max} = (1/2)(2M_{\max}+1)\theta$, $M_{\max} = 17$, $\theta = \arcsin\sqrt{1/2^n}$, and $n = 9$. Both $\langle P\rangle$ and $x$ are dimensionless. A thin solid curve represents $\langle P\rangle(\Theta, x)$ obtained by numerical calculation up to the 39th-order perturbation. Black circles represent results obtained by Monte Carlo simulations of the $n = 9$ case (nine qubits) with $M_{\max} = 17$. Each circle is obtained for $x = 2M_{\max}np = 306p$, where $p$ is varied from $p = 2.0 \times 10^{-3}$ to $p = 2.0 \times 10^{-2}$ at intervals of $\Delta p = 2.0 \times 10^{-3}$. In these simulations, we make 50 000 trials for taking an average.

approximation of $C_k(\Theta)$ with the 40th-order polynomial is reliable in this range, as shown in Fig. 4.) Hence, if we limit $x$ to $0 \le x \le 10.0$, the 40th-order perturbation is bounded to

$$0 \le |\frac{1}{40!}\bar{C}_{40}(\Theta)x^{40}| \le 1.24 \times 10^{-10}. \tag{35}$$

[From now on, we write $\langle P\rangle(\Theta, x)$ as the approximate form $\langle \bar{P}\rangle(\Theta, x)$ for convenience as far as this naming does not create any confusion.]

Let us investigate $\langle P\rangle(\Theta, x)$ obtained in Eq. (33) by numerical calculations. To confirm reliability of our perturbation theory, we compare the obtained $\langle P\rangle(\Theta, x)$ with results of Monte Carlo simulations of our model in Figs. 5 and 6. In these simulations, setting $n = 9$ (nine qubits), we fix $p$ and cause phase flip errors ($\sigma_z$ errors) at random in each trial. We take an average of $\langle 0|\rho^{(M)}|0\rangle_p$, the probability of observing $|0\rangle$ at the $M$th step $[M = 0, 1, ..., M_{\max}(= 17)]$, with 50 000 trials for each certain value of $p$. [Because $(\pi/4)\sqrt{2^9} = 17.7...$, we put $M_{\max} = 17$.]

Figure 5 shows $\langle P\rangle(\Theta, x)$ as a function of $x$ with fixing $\Theta = \Theta_{\max}$, where $\Theta_{\max} = (1/2)(2M_{\max}+1)\theta$, $M_{\max} = 17$, $\theta = \arcsin\sqrt{1/2^n}$, and $n = 9$. (Hence, the independent parameter is only $p$ actually.) At $x = 0$, there is no error in the quantum process and $\langle P\rangle$ is nearly equal to unity. As the error rate $x$ becomes larger, $\langle P\rangle$ decreases monotonically.

Figure 6 shows $\langle P\rangle(\Theta, x)$ as a function of $\Theta$ with fixing $p$. Because we use the variable $x = 2Mnp$ instead of $p$ in the perturbation theory, we have to rewrite $x$ as

$$x = 2Mnp = 2\Theta(\arcsin\sqrt{1/2^n})^{-1}np, \tag{36}$$

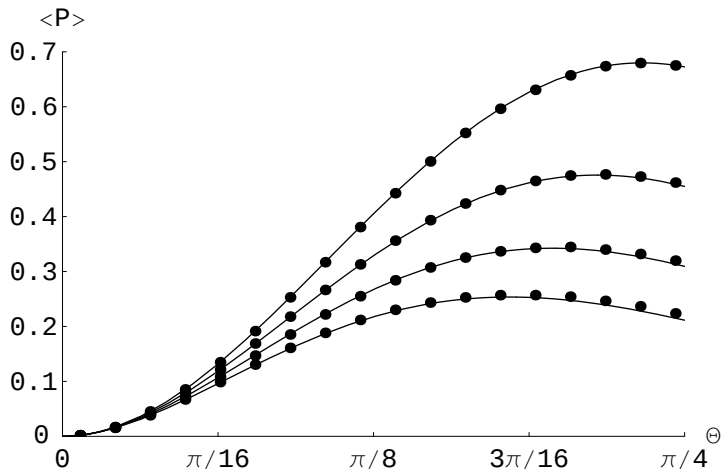


Figure 6: $\langle P\rangle(\Theta, x)$ as a function of $\Theta$ (radian) with fixing $p$. Both $\langle P\rangle$ and $\Theta$ are dimensionless. To estimate $\langle P\rangle(\Theta, x)$, we put $x = 2\Theta(\arcsin\sqrt{1/2^n})^{-1}np$, where $n = 9$. Four thin solid curves represent $p = 2.0\times10^{-3}$, $4.0\times10^{-3}$, $6.0\times10^{-3}$, and $8.0\times10^{-3}$ in order from top to bottom. Black circles represent results obtained by Monte Carlo simulations of the $n = 9$ cases (nine qubits). Each circle is obtained for $\Theta = (1/2)(2M + 1)\theta$, where $\theta = (\arcsin\sqrt{1/2^n})^{-1}$, $n = 9$, and $M \in \{0, 1, ..., M_{\max}(= 17)\}$.

which we obtain by substituting $\Theta = \lim_{n\to\infty} M\theta$ for $x = 2Mnp$ without taking the limit $n \to \infty$, and we give some finite $n$ to Eq. (36). In Fig. 6, we set $n = 9$ and plot curves with $p = 2.0 \times 10^{-3}$, $4.0 \times 10^{-3}$, $6.0 \times 10^{-3}$, and $8.0 \times 10^{-3}$ in order from top to bottom. We also plot results of the simulations. When we plot a result of the simulation for the $M$th step, we put

$$\Theta = (1/2)(2M + 1)\theta = (1/2)(2M + 1)(\arcsin\sqrt{1/2^n})^{-1}, \tag{37}$$

where $n = 9$ and $M \in \{0, 1, ..., M_{\max}(= 17)\}$. We obtain Eq. (37) from Eq. (13) and $\Theta = \lim_{n\to\infty} M\theta$.

From Fig. 6, we notice that the maximum value of $\langle P\rangle$ is taken at $\Theta < \pi/4$ for each $p$ and the shift becomes larger as $p$ increases. This fact means that $\Theta_{\rm th}(p_{\rm c}, P_{\rm th})$ becomes smaller than $\pi/4$, as $P_{\rm th}$ decreases. [We write $\Theta_{\rm th}(p, P_{\rm th}) = \lim_{n\to\infty} M_{\rm th}(p, P_{\rm th})\theta$ and $M_{\rm th}(p, P_{\rm th})$ represents the least number of the operations iterated for amplifying the probability of $|0\rangle$ to $P_{\rm th}$ under the error rate $p$.]

Finally, we compute $x_{\rm c}$ as a function of $P_{\rm th}$. We show the result in Figs. 2 and 3. We obtain $x_{\rm c}$ for $0 \le \forall P_{\rm th} \le 1$ as follows. We calculate $\tilde{\Theta}_{\rm th}(x, P_{\rm th})$ for given $P_{\rm th}$ varying $x$ from zero, where $\tilde{\Theta}_{\rm th}(x, P_{\rm th}) = \lim_{n\to\infty} \tilde{M}_{\rm th}(x, P_{\rm th})\theta$ and $\tilde{M}_{\rm th}(x, P_{\rm th})$ represents the least number of the operations to amplify the probability of $|0\rangle$ to $P_{\rm th}$ under given $x$. (We use Newton's method for obtaining a root of $\Theta$ for the equation $\langle P\rangle(\Theta, x) = P_{\rm th}$ for given $x$.) When $x$ becomes a certain value, we cannot find a root of $\tilde{\Theta}_{\rm th}(x, P_{\rm th})$ and we regard it as $x_{\rm c}$. By repeating this calculation for many points of $P_{\rm th}$, we obtain the curve shown in Figs. 2 and 3.

Using Eq. (21), a tangent at $P_{\rm th} = 1$ is given by

$$x_{\rm c} = c(1 - P_{\rm th}), \qquad c = -\frac{1}{C_1(\pi/4)} = \frac{8}{5}, \tag{38}$$

because $\tilde{\Theta}_{\rm th}(x_{\rm c}, P_{\rm th}) = \pi/4$ and $x_{\rm c} = 0$ for $P_{\rm th} = 1$. This means that the algorithm is effective for $2Mnp < (8/5)(1 - P_{\rm th})$ near $P_{\rm th} = 1$, as shown in Fig. 2. This result is similar to a work obtained by Bernstein and Vazirani [12], and Preskill [13], as explained in Sec. 1. Moreover, we notice $x_{\rm c} > -(8/5)\log_e P_{\rm th}$ near $P_{\rm th} = 0$ from Fig. 3.

# 5 Discussions

From Fig. 2, we find that the algorithm is effective for $x = 2Mnp < (8/5)(1 - P_{\rm th})$ near $P_{\rm th} = 1$, and this relation is applied to a wide range of $P_{\rm th}$ approximately. Thus, if we assume that $P_{\rm th}$ is equal to a certain value ($1/2 \leq P_{\rm th} \leq 1$, for example), we can expect that the algorithm works for $x = 2Mnp \leq O(1)$ ($x$ is equal to or less than some constant.) Hence, if the error rate $p$ is smaller than an inverse of the number of quantum gates $(2Mn)^{-1}$, the algorithm is reliable. If this observation holds good for other quantum algorithms, it can serve as a strong foundation to realize quantum computation.

After we studied decoherence in Grover's algorithm with a perturbation theory in Ref. [11], some other groups have tried similar analyses. Shapira *et al.* investigate performance of Grover's algorithm under unitary noise [17]. They assume the noisy Hadamard gate and estimate the success probability to detect a marked state up to the first order perturbation. Hasegawa and Yura consider decoherence in the quantum counting algorithm, which is a combination of Grover's algorithm and the quantum Fourier transformation, under the depolarizing channel [18].


### Acknowledgment

The author thanks Osamu Hirota for encouragement.


# A Proof of Eq. (29)

In this section, we prove Eq. (29), which we can rewrite in the form

$$f_k(\Theta) = \text{Const.}\Theta^{k+2} + O(\Theta^{k+4}) \qquad \text{for } k = 0, 1, .... \tag{39}$$

To put it more precisely, we can obtain the following relations in which Eq. (39) is included:

$$\begin{aligned} f_k(\Theta) &= a_0^{(k)}\Theta^{k+2} + a_1^{(k)}\Theta^{k+4} + a_2^{(k)}\Theta^{k+6} + ... \\ &= \sum_{j=0}^{\infty} a_j^{(k)}\Theta^{k+2(j+1)}, \end{aligned} \tag{40}$$

$$\begin{aligned} g_k(\Theta) &= b_0^{(k)}\Theta^{k} + b_1^{(k)}\Theta^{k+2} + b_2^{(k)}\Theta^{k+4} + ... \\ &= \sum_{j=0}^{\infty} b_j^{(k)}\Theta^{k+2j} \end{aligned} \tag{41}$$

$$\text{for } k = 0, 1, ...,$$

where $f_k(\Theta)$ and $g_k(\Theta)$ are defined in Eqs. (25), (26), (27), and (28).

We prove Eqs. (40) and (41) by mathematical induction. First, when $k = 0$, we obtain the following results from Eqs. (25) and (26):

$$\begin{aligned} f_0(\Theta) &= \sin^2 2\Theta = [\sum_{n=0}^{\infty} \frac{(-1)^n 2^{2n+1}}{(2n+1)!}\Theta^{2n+1}]^2 \\ &= 4\Theta^2 - \frac{16}{3}\Theta^4 + \frac{128}{45}\Theta^6 + ..., \qquad (42) \\ g_0(\Theta) &= \cos^2 2\Theta = [\sum_{n=0}^{\infty} \frac{(-1)^n 2^{2n}}{(2n)!}\Theta^{2n}]^2 \\ &= 1 - 4\Theta^2 + \frac{16}{3}\Theta^4 + .... \qquad (43) \end{aligned}$$

Thus, Eqs. (40) and (41) are satisfied for $k = 0$.

Next, assuming that Eqs. (40) and (41) are satisfied for some $k$, we investigate whether or not Eqs. (40) and (41) hold for $(k + 1)$. Let us consider Eq. (40) for $(k + 1)$. From Eq. (27), we obtain

$$f_{k+1}(\Theta) = \int_0^{\Theta} d\phi [f_k(\Theta - \phi)\cos^2 2\phi + g_k(\Theta - \phi)\sin^2 2\phi]. \qquad (44)$$

Here, we expand $\cos^2 2\phi$ and $\sin^2 2\phi$ as follows:

$$\begin{aligned} \cos^2 2\phi &= \sum_{j=0}^{\infty} c_j \phi^{2j}, \qquad (45) \\ \sin^2 2\phi &= \sum_{j=0}^{\infty} d_j \phi^{2(j+1)}. \qquad (46) \end{aligned}$$

From Eqs. (40), (41), (45), and (46), we can rewrite Eq. (44) in the form

$$\begin{aligned} f_{k+1}(\Theta) &= \int_0^{\Theta} d\phi \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} [a_i^{(k)} c_j (\Theta - \phi)^{k+2(i+1)}\phi^{2j} \\ &\qquad + b_i^{(k)} d_j (\Theta - \phi)^{k+2i}\phi^{2(j+1)}]. \qquad (47) \end{aligned}$$

Applying the following formula

$$\int_0^{\Theta} d\phi (\Theta - \phi)^i \phi^{2j} = \frac{i!(2j)!}{(i + 2j + 1)!}\Theta^{i+2j+1} \qquad (48)$$

to Eq. (47), we find that $f_{k+1}(\Theta)$ includes only terms of $\Theta^{k+3}$, $\Theta^{k+5}$, $\Theta^{k+7}$, .... Therefore, Eq. (40) holds for $(k + 1)$. Next, let us consider Eq. (41) for $(k + 1)$. From Eq. (28), we obtain

$$g_{k+1}(\Theta) = \int_0^{\Theta} d\phi [g_k(\Theta - \phi)\cos^2 2\phi + f_k(\Theta - \phi)\sin^2 2\phi]. \qquad (49)$$

Using Eqs. (40), (41), (45), and (46), we can rewrite Eq. (49) in the form

$$\begin{aligned} g_{k+1}(\Theta) &= \int_0^{\Theta} d\phi \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} [b_i^{(k)} c_j (\Theta - \phi)^{k+2i}\phi^{2j} \\ &\qquad + a_i^{(k)} d_j (\Theta - \phi)^{k+2(i+1)}\phi^{2(j+1)}]. \qquad (50) \end{aligned}$$

Applying Eq. (48) to Eq. (50), we find that $g_{k+1}(\Theta)$ includes only terms of $\Theta^{k+1}$, $\Theta^{k+3}$, $\Theta^{k+5}$, .... Therefore, Eq. (41) holds for $(k+1)$. Hence, from mathematical induction, we conclude that Eqs. (40) and (41) are satisfied for $k = 0, 1, ....$ This implies that Eq. (39) holds.

# References


[1] W.H. Zurek, 'Decoherence and the transition from quantum to classical', Phys. Today **44** (10), 36–44 (1991).

[2] W.G. Unruh, 'Maintaining coherence in quantum computers', Phys. Rev. A **51**, 992–997 (1995).

[3] G.M. Palma, K.-A. Suominen, and A.K. Ekert, 'Quantum computers and dissipation', Proc. R. Soc. London, Ser. A **452**, 567–584 (1996).

[4] I.L. Chuang, R. Laflamme, P.W. Shor, and W.H. Zurek, 'Quantum computers, factoring, and decoherence', Science **270**, 1633–1635 (1995).

[5] P.W. Shor, 'Scheme for reducing decoherence in quantum computer memory', Phys. Rev. A **52**, R2493–R2496 (1995).

[6] A.M. Steane, 'Error correcting codes in quantum theory', Phys. Rev. Lett. **77**, 793–797 (1996).

[7] A.R. Calderbank and P.W. Shor, 'Good quantum error-correcting codes exist', Phys. Rev. A **54**, 1098–1105 (1996).

[8] L.K. Grover, 'Quantum mechanics helps in searching for a needle in a haystack', Phys. Rev. Lett. **79**, 325–328 (1997).

[9] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, 'Tight bounds on quantum searching', Fortschr. Phys. **46**, 493–505 (1998).

[10] A. Ambainis, 'Quantum lower bounds by quantum arguments', e-print quant-ph/0002066.

[11] H. Azuma, 'Decoherence in Grover's quantum algorithm: Perturbative approach', Phys. Rev. A **65**, 042311 (2002); H. Azuma, Phys. Rev. A **66**, 019903(E) (2002).

[12] E. Bernstein and U. Vazirani, 'Quantum complexity theory', SIAM J. Comput. **26**, 1411–1473 (1997).

[13] J. Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, (California Institute of Technology, 1998), Chap. 6.
http://www.theory.caltech.edu/~preskill/ph229

[14] A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, 'Approximate quantum Fourier transform and decoherence', Phys. Rev. A **54**, 139–146 (1996).

[15] S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio, and J.I. Cirac, 'Improvement of frequency standards with quantum entanglement', Phys. Rev. Lett. **79**, 3865–3868 (1997).

[16] M.A. Nielsen and I.L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000), Sec. 8.3.3.

[17] D. Shapira, S. Mozes, and O. Biham, 'Effect of unitary noise on Grover's quantum search algorithm', Phys. Rev. A **67**, 042301 (2003).

[18] J. Hasegawa and F. Yura, 'Theoretical analyses of quantum counting against decoherence errors', e-print quant-ph/0503202.